1.7 Commencement of Operation

As noted in Section 1.3, it is prudent to use a phased implementation to minimize the impact of the inevitable problems. Specifically, the plan should keep the prior traditional system in operation during development, to provide a fallback option. If the organization that initiated the implementation of the EC system has many smaller trading partners, a small subset of them should be selected for readiness testing, and then operational use. After a reasonable trial period, additional trading partners can be converted to the EC system.

Here is a checklist of points to consider when planning the implementation:

1) Use stepwise testing to confirm that the hardware, software, and procedures work correctly by conducting tests in the following order:
(a) application to EDI system;
(b) EDI system to application;
(c) EDI system to EDI System;
(d) application to application.

2) When the system design has stabilized, conduct a training program for operating personnel of both trading partners.

3) Begin operation on a limited scale as discussed above; broaden the scope as confidence grows.

1.8 The EC System Contingency Plan

Just as with conventional data processing systems, it is essential to construct and maintain a contingency plan. The plan should enable the trading partners to respond to, and recover from, system failures ranging from the failure of individual system elements to catastrophic events that destroy buildings and their contents. Contingency planning for an EC system is complicated by two factors: (a) the dependency of trading partners on electronic interchanges, and (b) the reduction in human oversight.

The TPA should describe how partner contingency plans will provide for factors like these:

1) How and under what circumstances a trading partner notifies other partners of service interruptions.

2) What modifications, if any, will be made to timeliness requirements if there is a service interruption.

3) The extent to which one partner will assist another partner to recover data lost in a disaster, and the terms under

which the assistance is provided.

The TPA should also define how and when trading partners will conduct joint contingency tests. See Section 3.9 for more about this.

1.9 Management of Electronic Documents

It is important to be sure that documents that are in electronic form are available to comply with legal retention and disaster recovery requirements, and to satisfy auditor needs. However, EC systems can make it more difficult for a data owner to control access to data held by others. To ensure the ability to recover from failures promptly, EC systems typically store copies of a given electronic document in more than one place. For example, the record of a confidential price quotation might exist in a sender's application on-line and back-up files, the sender's EDI system back-up files, the value-added network's (VAN's) back-up files, the recipient's EDI system back-up files, and one or more of the recipient's application files. The TPA should address the questions of data ownership, and how long nonowners are permitted to retain data to protect the property rights of trading partners. See Section 3.7 for more about electronic document management.

1.10 Selecting a Network

Trading partners need to be connected to a data communications network that can transmit their EDI transaction sets. Selection of a network is important because it will influence the performance of the trading partnership in two quite different ways:

1) The technical characteristics of the network, its traffic handling capacity, its data protection and data integrity, and its reliability/availability must meet the needs of trading partners.

2) VAN status-reporting services can be used to support security and control objectives.

Network considerations are discussed in Sections 2.10, 2.11, and 3.5. It is important to identify the network arrangement that will provide the best overall cost/performance for the trading partners including security and control considerations. If a third party network is used, the network agreement that the trading partners sign should include provisions such as the following to meet the requirements of the trading partners:

1) Physical and logical controls over access to trading partner messages by both network personnel and outsiders.

2) Provisions for administration by the network of trading

partner identifications (IDs) and passwords used to control access to the network.

3) Performance warranties of network availability, accuracy of message transmission, and message delivery time.

4) Retention of messages to permit recovery from disasters.

5) Retention of logs to permit subsequent audit of activity.

The specific details of the network usage should be fully defined in an appendix to the TPA.

2. IDENTIFICATION OF ELECTRONIC COMMERCE SYSTEM RISKS

2.1 Introduction

This chapter discusses operational aspects of EC and EDI that lead to the unique risks of EC systems. If the initial risk assessment of an EC system is inadequate, some risks may be ignored or understated, resulting in inadequate security measures. As a result, excessive protection may be provided against other risks, resulting in wasted resources. The information in this chapter can be used to structure the risk analysis to be sure that all potential risks are evaluated. Section 2.16 discusses general risks that are not specific to EC systems, but that should be included in the risk analysis.

2.2 Basic EC and EDI Operations

The objective of EC is to minimize or eliminate paper documents and routine human participation in processing, to reduce costs and improve performance. For example, in a traditional paper-based trading process, personnel at government agency ABC compose and print a purchase order and cause funds to be reserved in the agency's financial system. The purchase order is reviewed and signed by a contracting officer, and mailed to company XYZ. At company XYZ, a salesman verifies price, quantity, and shipping date. An order entry clerk uses a computer workstation to enter the purchase order information into the XYZ order entry system.

Case Study: Experience shows that for typical business systems such as the example above, about 70% of the mismatches between documents, (for example, the price shown on a purchase order and on the subsequent invoice), are caused by keystroke errors when data are entered from paper documents. The direct cost to correct these relatively simply errors ranges from about $7.50 to $25.00 each. Consequential costs are likely to be much higher if the errors are not detected promptly. EC systems have the potential to eliminate most of these errors.

When ABC and XYZ agree to use EC, the purchase order document and most of the human processing are eliminated. A contracting officer at agency ABC releases the purchase order from a computer workstation. Under some circumstances, a routine purchase order might be generated automatically in response to a message from an inventory control system, when the product needed is obtainable as a delivery order under an existing contract. The purchasing system then transmits the purchase order information to ABC's EDI computer system while automatically informing the agency's financial system. The EDI system translates the information into a standard EDI transaction set, and passes it to a communications network used by ABC and XYZ.

The communication network puts the transaction set in XYZ's "mailbox." Later XYZ's EDI computer retrieves the transaction set from its "mailbox." The EDI computer then translates the transaction set from the EDI standard format into a data file record that is compatible with XYZ's order entry system, and passes the file to the order entry system. The order entry system automatically performs the various checks. If there is an exception condition, for example an invalid part number, human intervention is triggered. Otherwise, the order is processed automatically. For example, the order entry system might send an Advance Shipping Notice transaction set back to ABC with full details of how the order is being processed.

2.3 Defining Threat, Risk and Security

A threat can be thought of as a potential event that has some non-zero probability of occurrence, and which causes a loss when it occurs. Risk, defined in Section 1.4 as the likelihood of loss, may be considered with respect to the occurrence of a particular threat. The term security is used in its broadest sense in this report. A security technique is any action taken to reduce the risk associated with a particular threat occurrence. A security technique may be an application of a policy or procedure, use of a hardware device, or implementation of a software feature.

The boundary between operational and security issues cannot be sharply defined, and the reader may feel that a "security technique" described here is simply "good system design practice." Perhaps the best distinction is between techniques required simply to make the EC system work correctly when all the system elements perform exactly as expected, and the techniques required for acceptable real-world operation when, inevitably, performance is not flawless.

Indeed, an EC system can be implemented without applying the "good security practices" described in this report. If testing is inadequate, the system may appear to function satisfactorily. If nothing can go wrong at any time, good security practices are not required. However, both analysis and experience suggest that the threats described in this report may occur. These occurrences will have a significant negative impact on EC systems unless good security practices have been implemented.

Note that the mere existence of a threat is not, of itself, sufficient reason to install a security technique. The need for a technique depends on the magnitude of the loss it is expected to reduce or eliminate. The magnitude of the loss resulting from a threat occurrence depends on several factors:

1) the anticipated rate of occurrence of the threat;

2) whether the threat occurrence is accidental or deliberate; there may be a greater loss if an EDI message is maliciously and carefully altered than if it is accidentally and randomly changed;

3) the type of transaction: information versus action;

4) the volume of transactions per day exposed to the threat;

5) the urgency of the transactions;

6) the monetary value of the transactions; and

7) the dependence of other processing systems on the system being considered.

It is not a sound management practice to expend resources protecting against threats that will not have a significant loss impact, i.e., risk. Since the relative importance of threats and vulnerabilities is not always obvious, it is important to conduct an adequately detailed risk analysis as described in Section 1.4 to ensure that security resources are allocated wisely.

Some EC risks are inherent in the basic concept of EC. Others are specific to the five individual elements of EC systems as defined in Section 2.5. The following are basic objectives for the security of EDI transaction sets:

1) Content Integrity. Content cannot (easily) be altered, or detection of alteration is assured.

2) Sequence Integrity. Detection of missing, duplicated, or out-of-sequence transaction sets is assured.

3) Content Confidentiality. Depending on the sensitivity of the contents, the probability of an unauthorized disclosure is acceptably low.

4) Sender Authentication. The recipient can verify the originator. Note: The term "sender" is used here to mean an organization, for example a government agency, or a corporation. However, in some instances there may be an additional requirement to authenticate the individual by name who "signed" (authorized the dispatch of) a transaction set.

5) Recipient Authentication. The sender can verify that the intended recipient received the document.

6) Timely Delivery. EC system reliability ensures that transmission of transaction sets from sender to recipient meets timeliness goals.

7) Exclusive Delivery. A transaction set should only be

delivered to the intended recipient.

Note the difference between using either prevention or detection to achieve these objectives. In many cases, detection is significantly cheaper than prevention, but it requires a recovery action when an error or exception condition is detected. The cost of recovery should be added to the direct cost of the detection method to determine the total cost. Preventative measures should only be adopted to achieve a security objective when it can be shown that the risk reduction warrants the extra cost. It should be noted that it is difficult to detect unauthorized disclosure of information. Prevention using cryptography may be less costly and more reliable than detection.

Much of EC security focuses on the need to find automated substitutes for the human oversight that characterizes traditional paper-based business transactions. There are four generally applicable EC system good security practices that support this objective:

1) Automated Acknowledgment. As transaction sets pass from the sender's application to the recipient's application, acknowledgments are passed back and processed automatically. Each system element in the transmission path maintains a log of the transaction sets it is processing. Each log record includes a note of the time by which acknowledgment must be received. A negative acknowledgment (the transaction set is invalid and was rejected) or failure to acknowledge within the specified time limit triggers an exception condition requiring appropriate resolution, possibly involving human intervention. See Section 3.2 for a detailed discussion of this topic.

2) Maintenance of Audit Trails and Archival Records, and Electronic Document Management. Since the elimination of paper records is an essential characteristic of EC systems, care must be taken in the design and operation of EC systems to ensure that the electronic documents that the systems create and maintain will be accepted by law courts and auditors as the equal of equivalent paper documents that are "records kept in the ordinary course of business."

3) Careful Definition of All Aspects of the Transactions. The EDI transaction set standards developed by the X12 Committee serve to define the technical structure of the EDI messages passed between trading partners. These standards should be used in EC system design to the extent possible. Well-drafted individual trading partner agreements (TPAs) define in detail how each transaction set is to be processed, and the liability of each partner regarding all abnormalities.

4) Authentication. Where warranted by the level of risk, security techniques are employed to give trading partners confidence that individual transactions are authentic. This may include

the use of authentication codes and digital signatures with transaction sets. See Sections 3.3.5 and 3.3.6 for more about this.

In the sections that follow, specific implementations of these recommended practices are discussed.

2.4 General EC System Security Requirements

1) Coordination between partners must be complete.

Coordination between trading partners must be complete to protect against unrecognized differences in interpretation of operating modes, meanings of transaction sets, responsibility for exception detection, cryptographic key incompatibility, differences between printed information and electronic data, etc.

2) The TPA must adequately define "terms of sale" and other duties and obligations of the partners; legal liability should be adequately defined and assigned.

A traditional printed purchase order form includes terms of sale. Because of the nature of EC, the terms of sale and other duties and obligations of the trading partners are defined in advance before individual transactions take place; they are included by implicit reference in each transaction. Since EC introduces new elements into the conduct of business and reduces human review and approval of transactions, it is essential that the TPA be complete and unambiguous about terms and conditions that apply to transaction sets. Similarly, the TPA must adequately define and assign responsibilities for unsatisfactory operating results causing unexpected liability.

3) EC system records must be adequate to satisfy legal requirements for their trustworthiness.

It is generally recognized by courts that records "maintained in the ordinary course of business" may be admitted as evidence. Since many if not all the records of EC transactions are stored electronically rather than on paper, it is important to be sure that the way in which such records are structured, created, recorded and stored will allow them to be accepted as trustworthy.

4) Implementation should be complete and effective to avoid conflicts between electronic documents and printed material.

Care must be taken with the details of the implementation to anticipate and resolve possible ambiguity in the interpretation of EC transactions. The TPA and the methods used to create and maintain computerized records of prices, part numbers and descriptions, and the like should completely replace paper records similar factors. Otherwise, there is a risk that a trading partner will use obsolete

information from a paper document, for example, an out-of-date catalog or price list, to compose a transaction set. Ideally, information of this sort should be exchanged using EDI and incorporated automatically into the applications using the information.

5) EC system reliability must satisfy trading partner requirements for timely processing.

The designers and users of an EC system have expectations about the reliability of the hardware and software. Hardware and software failures, and human errors may result in (a) processing delays, (b) lost transaction sets, logs, and data files, and (c) unauthorized disclosure of information. The reliability expectations should be explicitly defined; the details of the hardware and software design and implementation, and the operating procedures, should ensure that these expectations are met.

6) Audit of EC systems should be effective.

Audit of EC systems must be adequate in scope, depth, frequency and technical competence to ensure timely detection of material deficiencies. See Section 3.8 for a discussion of this topic.

7) Transaction set authentication must be commensurate with the risk of repudiation or deception.

Because paper documents and human oversight are both minimized or eliminated, there is a risk that a trading partner may claim that a transaction set was not sent or received, or that the content of a transaction set is different than understood by another partner. This is sometimes referred to as repudiation. The EC system design should include features to minimize:

(a) uncertainty about the flow of transaction sets between trading partners, and

(b) the possibility that changes (both accidental and deliberate) to a transaction set will not be detected.

The term "non-repudiation" was devised by technical experts to characterize EC systems that employ cryptographic techniques in order to assure that a trading partner could not deny transmission or reception, or deny specific message content. The term was used because of the assumption that one could not repudiate cryptographically authenticated transaction sets. In fact, a trading partner is always free to repudiate a transaction set regardless of the authentication technique used. It is more accurate to say that repudiation is discouraged with use of an authentication technique that provides evidence difficult to refute.

Ultimately, the authentication characteristics of a transaction set simply contribute to the weight of the evidence in a legal action,

but the courts decide if the repudiation of a transaction set will be upheld or overturned. Thus, we conclude that the strength of the authentication method used by an EC system should be commensurate with the risk of repudiation. Sections 3.3.5 and 3.3.6 discuss authentication techniques, and Section 3.2 describes the use of acknowledgments to support the objective of non-repudiation.

8) Only authorized accesses to EC systems must be permitted.

Unauthorized access to computer systems is a significant problem in many organizations. Such access may be obtained from inside or outside the organization, e.g., via compromise of passwords and identifications, or compromise of telephone numbers and communications equipment. Poorly protected databases and access points for maintenance and computer system management personnel are vulnerabilities that can be exploited. Additional information on protective techniques may be found in NBS SP 500-137, Security for Dial-Up Lines; NIST SP 500-171, Computer User's Guide to the Protection of Information Resources; FIPS PUB 112, Standard on Password Usage; and FIPS PUB 181, Automated Password Generator.

Unauthorized accesses may be for the purposes of sabotage or for obtaining sensitive data. Data in trading partners' systems may have value to parties unauthorized to receive them. These data are vulnerable while in the sender's or recipient's applications and while being interchanged through EDI. Types of data subject to compromise may include personal data such as salaries and records of health conditions, and trade secrets such as bids in response to requests for quotes and plans for new business initiatives.

9) Passive wiretapping should be prevented for a system at risk.

There is no infallible way to detect passive wiretaps. Consequently, prevention is a more reliable safeguard than detection, but the cost of prevention is justified only if there is a significant risk. The risk of interception depends on two factors: (a) the character of the contents of a transaction set as a motivation to intercept it, and (b) the extent to which the transmission path is vulnerable to wiretapping. In other words, the value to an intruder of the information obtained from a wiretap must be perceived by the intruder to be significantly higher than the cost (including the risk and consequences of being caught in the act) of installing and operating the wiretap. Vulnerability alone does not automatically create a high risk and justify the cost of prevention.

Practically speaking, it is very difficult to identify a particular organization's transmissions in the stream of transmissions in a multi-user network unless one has full access to network facilities. Consequently, wiretaps are most likely to be placed on or near a trading partner's premises where circuits can be accessed and identified. If the nature of the information being transmitted

suggests that wiretapping is a serious threat, then care should be taken to control access to telephone closets and other locations where circuits are accessible. Encryption of messages raises the cost of interception sharply.

10) Techniques should be used against active wiretapping when needed.

The term "active wiretapping" is used here to refer to the act of intercepting a transaction set, making changes to the transaction set intended to benefit the intruder, and then inserting the transaction set back into the data stream. Similar to passive wiretaps, the risk of active wiretaps depends on the extent to which a potential intruder perceives that the benefit of making a modification outweighs the cost.

Note that the cost to modify a transaction set is significantly higher than mere interception. Deliberate modification implies that specific transaction sets are being targeted. In most cases it would be quite difficult technically to locate a specific transaction set, intercept it, modify it, and then insert it back into the data stream without causing an error condition or otherwise having the modification activity detected.

One location at which intentional modification could occur is at a VAN used as part of the process transmitting the transaction set to trading partners. VAN users should assure themselves that VAN security procedures and contractual arrangements with the VAN significantly lower this possibility.

Software analyses on received data that checks for reasonableness of values and compares values in the same fields of different messages from the same trading partner may be used as aids in the detection of alterations, both deliberate and accidental. Techniques for prevention, in addition to detection, may be employed if active wiretapping is a serious threat and satisfactory methods of detection cannot be devised. Cryptographic techniques for authentication and confidentiality also protect against transaction set modification.

11) Protective measures should be implemented against system sabotage and natural disasters that could disrupt operations.

Once trading partners have abandoned the traditional processing systems, their strong dependence on EC makes the system an attractive sabotage target. Similarly, a natural disaster such as a flood, fire, or power or telephone outage could disrupt operations significantly. It is important to provide effective physical protection for EC system facilities, and to maintain effective contingency plans.

2.5 Risks Specific to the Five Elements of an EC System

EC is characterized by the automated transmission of transaction sets between the computerized business applications of trading partners using five basic elements. Some risks apply to specific elements of an EC system. The five elements are as follows:

1) The Sender's Application. The computer application that generates EDI documents, for example, a procurement system that generates purchase orders.

2) The Sender's EDI System. The computer and communications system that receives a document from a sender application, translates it into a standardized EDI format, and passes it to the network.

3) The Network. The communications facility that passes EDI transaction sets from the sender's EDI system to the recipient's EDI system.

4) The Recipient's EDI System. The computer and communications system that receives an EDI transaction set from the network, translates it into a compatible format, and passes it to a recipient computer application.

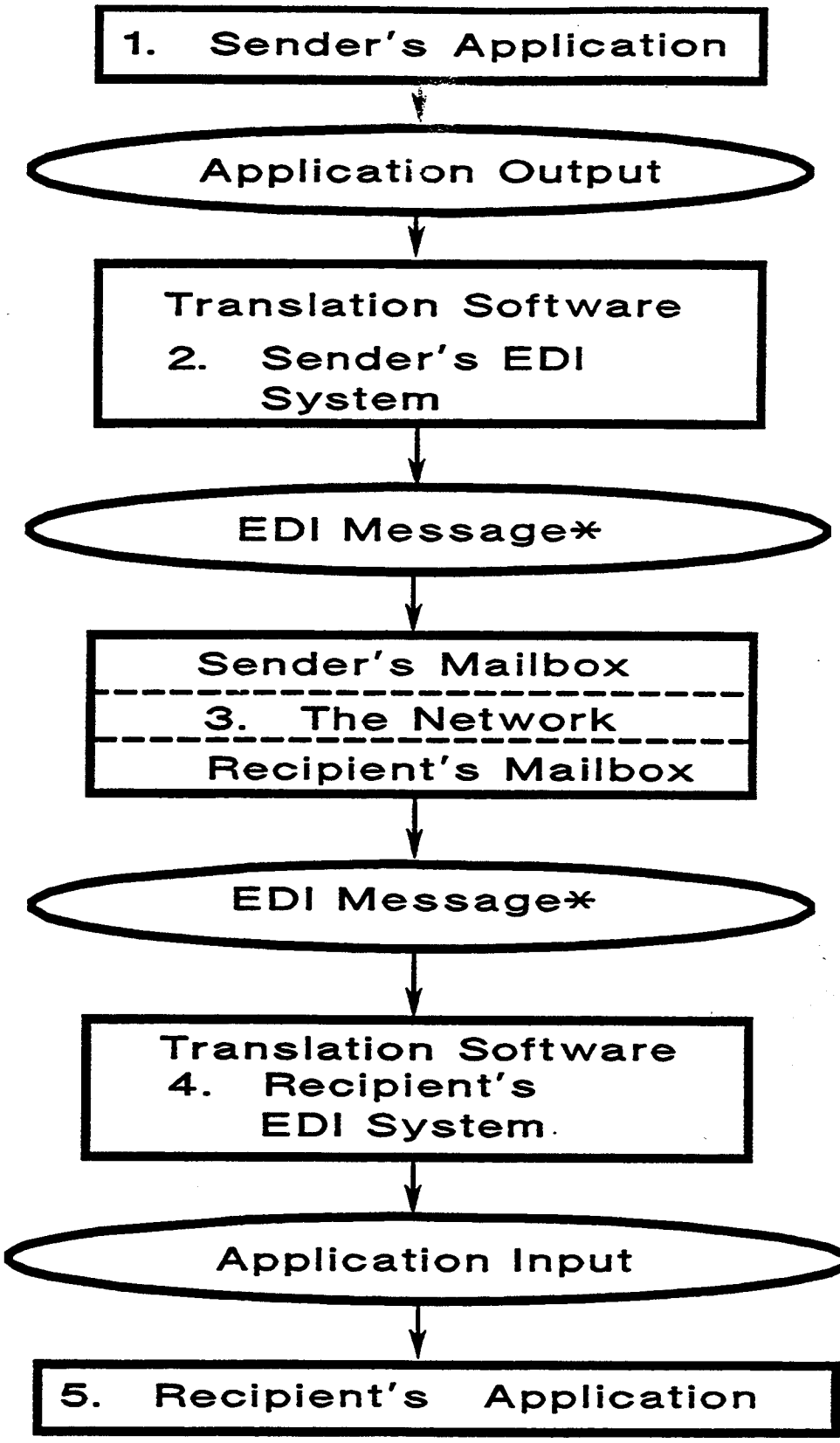
5) The Recipient's Application. A computer application that receives and processes the information in an EDI transaction set, for example, an order entry system.

Figure 1, p. 28, shows the relationship among these five elements graphically. Each of these elements and the associated risks are described in more detail in the subsections that follow.

2.6 The Sender's Application

A typical sender's application accepts inputs, maintains a database, and generates output. In a paper-based system, some of the output is traditional business documents. These documents are transmitted to trading partners by a number of different methods such as mail, courier services, fax, and telex. In EC, the sender's application sends output to the sender's EDI system for processing.

For example, a sender's procurement system maintains a list of approved vendors, accepts purchase order information, initiates purchase orders, maintains a database of outstanding purchase orders, and generates purchase order transactions that it passes to the sender's EDI system. Each transaction in the output file must contain all the information required by the EDI system to compose the EDI transaction set.



*: One or more transaction sets.

Figure 1. The Five Elements of an EC System.

Fully developed EC systems will interconnect applications to eliminate routine human intervention where possible. For example, an inventory control system will detect the need to replenish the stock of a purchased item and send a "requisition" to the purchasing system. The purchasing system will consult its database and identify vendors of the item, and pricing information. It may generate a purchase order transaction automatically if it can associate the needed item with an open contract from which deliveries may be obtained. Otherwise, it could inform an inventory specialist of the need to issue a request for quotes. (For certain well-defined stock items, the issuance of a request for quotes could be done automatically as well). Ideally, the purchasing system receives pricing and part number update data from vendors as EDI transaction sets, and updates its database automatically.

2.7 Potential Risks of the Sender's Application

Hardware and software failures of the sender's application cause the following risks:

1) The content of a transaction is incorrect.

2) A transaction is not initiated as expected, and is not passed to the EDI system.

3) A transaction is misaddressed, and does not go to the intended recipient.

4) A duplicate transaction is generated and sent to the recipient.

5) A failure to reconcile transactions with the EDI system's list of transaction sets processed is not detected.

2.8 The Sender's EDI System

The sender's EDI system receives transactions from the sender's application, usually in the form of flat files of transaction records. While the details of the implementation may vary, the typical sender's EDI system has two major computerized parts: a translation program, and a network interface.

The function of the translator is to convert the output from the sender's application into standard EDI message formats called transaction sets. Each transaction set defines the precise arrangement of the contents of an EDI message. For example, the X12 Committee has defined a number of transaction set standards. Each standard is identified by a number and name. Some typical X12 transactions sets are: 810 Invoice; 820 Payment Order; 840 Request for Quotation; and 997 Functional Acknowledgment. Each transaction

set is made up of data segments, each of which consists of one or more data elements. The structure of the X12 standards allow data segments and data elements to be used in more than one transaction set. The Data Interchange Standards Association (DISA) Publications Catalog, issued annually, includes an excellent summary of these concepts, and lists the transaction set standards. DISA serves as the secretariat for the X12 Committee.

The translator creates a transaction set, for example an 850 Purchase Order, by converting transaction data fields in the application's flat file into the required transaction set data elements and data segments. The translator follows mapping information supplied to it by its designers. The X12 standards allow two or more transaction sets of the same type going to the same recipient to be assembled into what is called a functional group. Any number of functional groups going to the same recipient can be assembled into a single message using within what is called the interchange envelope. The translator includes in the interchange envelope the information needed to identify the recipient to the network.

The network interface passes the transaction sets to the network, and maintains appropriate transaction logs to ensure that all transaction sets are delivered to the designated recipient.

2.9 Potential Risks of the Sender's EDI System

The possibility of hardware and software failures of the sender's EDI system, and misfeasance or malfeasance of EDI system personnel result in the following risks:

1) A error in translating a transaction into EDI format (incorrect or incomplete information) is not detected and corrected. Thus, an invalid transaction set is sent to the network.

2) A valid transaction set is corrupted before being passed to the network.

3) An incorrect recipient identification is added to a valid transaction set before it is passed to the network.

4) A valid transaction set is created from a sender's application transaction, but is not queued for transmission.

5) A valid transaction set is transmitted more than once.

6) The expected acknowledgment of a transaction set is not received within the stipulated time, but an exception condition is not generated.